TRAFIKVERKET

TRAFIKVERKET

GDPR & Digitalisering

I bygg och anläggning
Uppdaterad 2022-12-01

Per Tuvall, Dataskyddsombud

Per Tuvall

Dataskyddsombud på Trafikverket

Certifierad CPP/EU-DPO
Immaterialrättsfrågor & öppna licenser
Egen utbildningsverksamhet

Tidigare erfarenheter

Trafikverket	IT-Strateg
Trafikverket	Teknisk Kundansvarig
Trafikverket	Teknisk Förvaltningsledare
Lan Assistans	Projektledare/specialistkonsult kommunikation & säkerhet
Atea/Martinsson	Specialistkonsult datakommunikation & säkerhet
UKD	Kursansvarig programmeringslärare
Umeå Universitet	Civilingenjör Teknisk datavetenskap

per.tuvall@trafikverket.se
https://www.linkedin.com/in/pelpet/

6

Vi förvaltar en värdefull anläggning

Statens vägnät, 10000 mil

Statens järnvägsnät, 1400 mil

Bokfört värde ca 425 miljarder kr
Återanskaffningsvärde för anläggningen är cirka 2 250 miljarder kr

Bokfört värde enligt Trafikverkets årsredovisning 2020. Återanskaffningsvärde enligt Underhålls affärsplan 2018. Årlig drift- och underhållskostnad är ca 25 miljarder fördelat över ca 500 kontrakt. Total budgetram 75 miljarder. Antal anställda 10000.

7

TRAFIKVERKET

Anläggningen bär historia och kultur

Arbete på Ostkustbanan, dubbelspår mellan Stockholm och Uppsala vid Alsike. Ca 1900. Bildkälla: Wikipedia

8

TRAFIKVERKET

Sveriges vägnät

- 98 500 km statliga vägar
- 42 300 km kommunala vägar
- 74 000 km enskilda vägar med statsbidrag
- Ett stort antal enskilda vägar utan bidrag (mycket skogsbilvägar)
- 16 600 broar, ett tjugotal tunnlar och 39 färjeleder
- Av det statliga vägnätet är 18 400 km grusväg (ungefär 20 procent av den totala väglängden).

9

TRAFIKVERKET

Sveriges järnvägsnät

Sveriges järnvägsnät är drygt 16 500 spårkilometer. Av detta förvaltar Trafikverket infrastrukturen för drygt 14 100 spårkilometer. Den allra största delen, omkring 80 procent, är elektrifierad järnväg.

10

TRAFIKVERKET

TRAFIK ANALYS

Transportarbete i Sverige 2000–2020

Persontransportarbetet under 2020 var 121,4 miljarder personkilometer, eller 1 170 mil per invånare.

88% vägtrafik

8% järnväg, spårväg och tunnelbana

3% luftfart

1% sjöfart

Godstransportarbetet under 2020 var 102,5 miljarder tonkilometer, eller 9 900 tonkilometer per capita.

52% vägtrafik

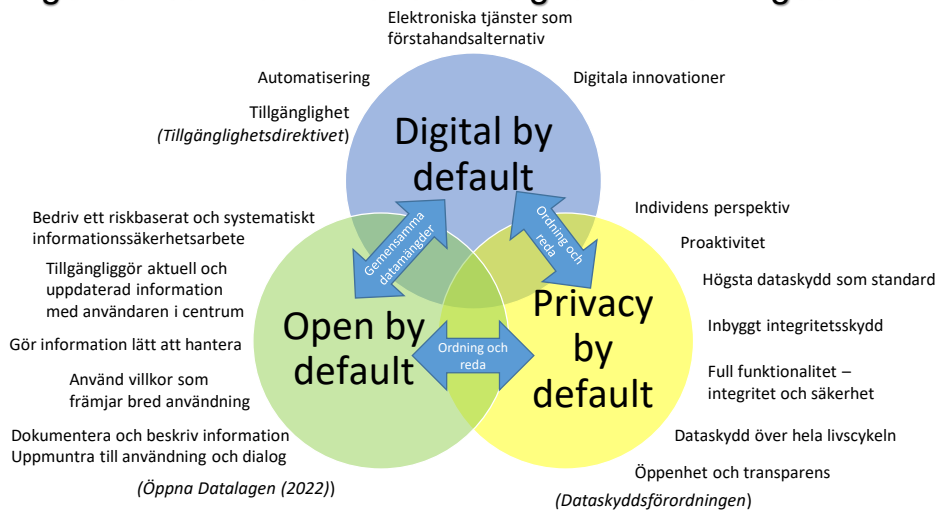
28% sjöfart

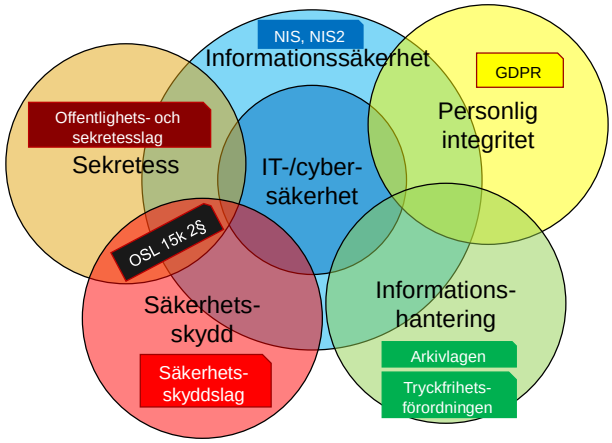
20% bantrafik

<0,1% luftfart

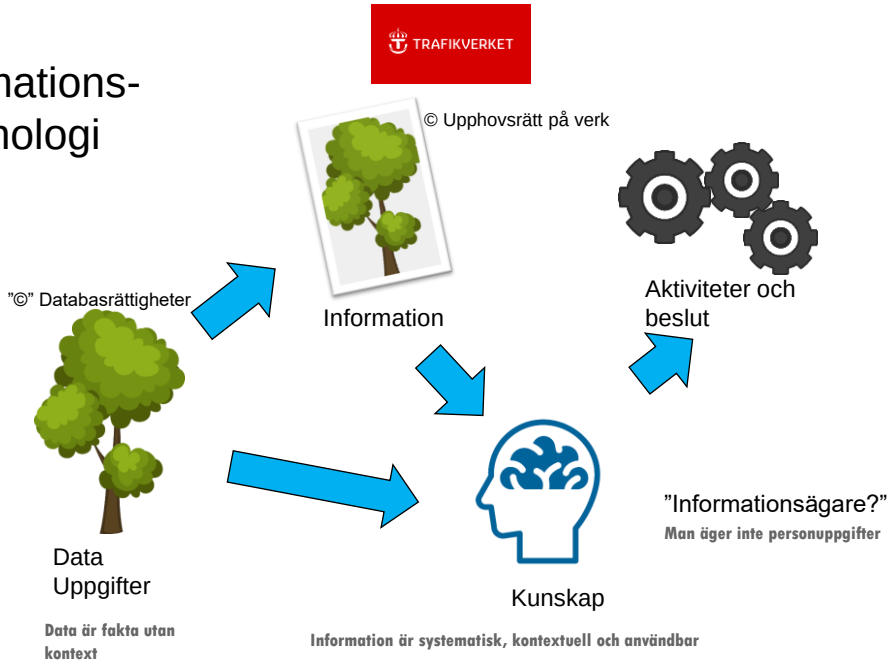
Källa: Trafikanalys, Transportarbete i Sverige 2000–2020, Statistik 2021:33

Digitaliseringen av samhället kräver ett digitalt förhållningssätt





Informations-terminologi



Den regulatoriska miljön kring molntjänster är utmanande

När man använder en leverantör så röjer man uppgifter för leverantören. Röjandet måste vara lagligt.

Sekretess OSL

Digital suveränitet

Dataskydd GDPR

Har man rådighet över information och verksamhet hos en utländsk leverantör?

Schrems-II-domen påtalar att amerikansk övervakning är oförenlig med Europakonventionen.

GDPR - Legal kontext

Förordning
EU-Lag: Gäller direkt i hela EU

Skäl / Recitals (173 st)
Utgör motiveringen till lagen och kan användas i tolkning och bedömning.

Artiklar (99 st)
Principerna (art 5)
Tillämpningsområde (art 2)
Rättslig grund (art 6)
Information, rättigheter, tredjelandsöverföring, etc
Hur principerna skall efterlevas.

Dataskyddslagen – svensk lag
Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

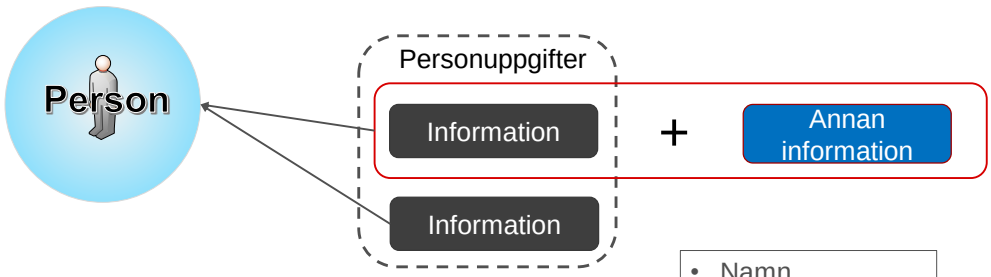
Europeiska datatillsynsmannen EDPS
Granskar EU-institutioner

Europeiska dataskyddsstyrelsen EDPB
Samordnar tillsynsmyndigheter

IMY
Svensk tillsynsmyndighet

Tillsynsbeslut från alla nationella

Domstolar
Civilrättslig prövning



- Namn
- Telefonnummer
- Epost
- Bild
- Registeringsnr
- IP-adress
- etc.

Varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad *en registrerad*), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet

Källa: Dataskyddsförordningen

Personuppgiftsbehandling
Allt man gör med personuppgifter tills de är raderade

Integritets-lagar

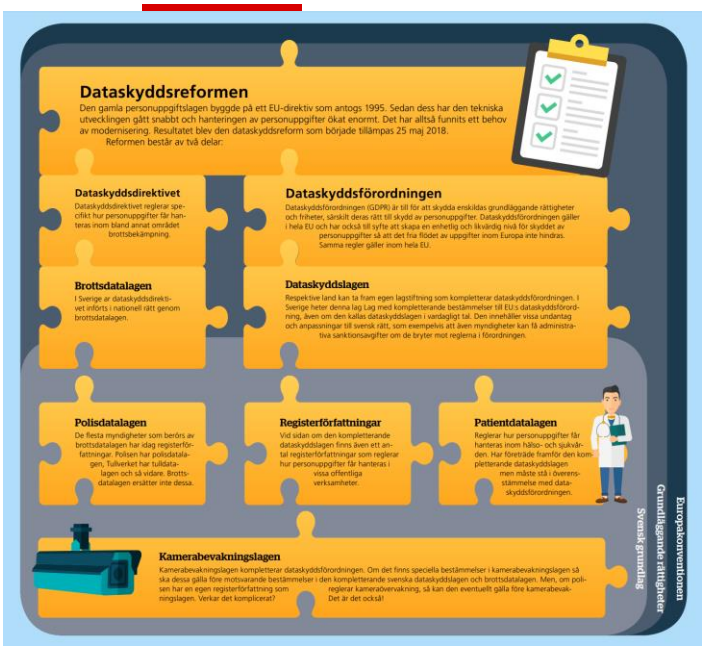


Bild från IMY. Länk.

TRAFIKVERKET

GDPR Artikel 5 - *Principer för behandling av personuppgifter*

1. Vid behandling av personuppgifter ska följande gälla:
   a) laglighet,
      korrekthet (*rättvis*) och öppenhet
   b) ändamålsbegränsning
   c) uppgiftsminimering
   d) korrekthet (*riktig*)
   e) lagringsminimering
   f) integritet och konfidentialitet
2. Ansvarsskyldighet

Artikel 6
Samtycke
Avtal
Rättslig förpliktelse
Skydd för grundläggande intressen
Uppgift av allmänt intresse och myndighetsutövning
Efter en intresseavvägning

Dokumentation är efterlevnad

Max Schrems

Maximilian Schrems är en österrikisk integritetsaktivist som har drivit flera kampanjer mot Facebook. Har grundat NOYB - European Center for Digital Rights

NOYB = *None Of Your Business*
https://noyb.eu/

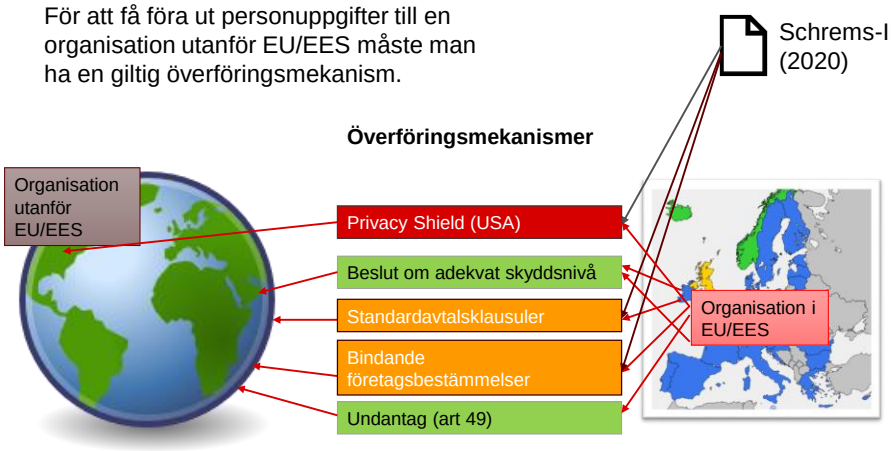
Bildkälla: Wikipedia

Tredjelandsöverföringar

GDPR kapitel 5 (artikel 44 – 50)

För att få föra ut personuppgifter till en organisation utanför EU/EES måste man ha en giltig överföringsmekanism.

”FISA 702 och Exekutiv Order 12333 är oförenliga med Europakonventionen om mänskliga rättigheter”

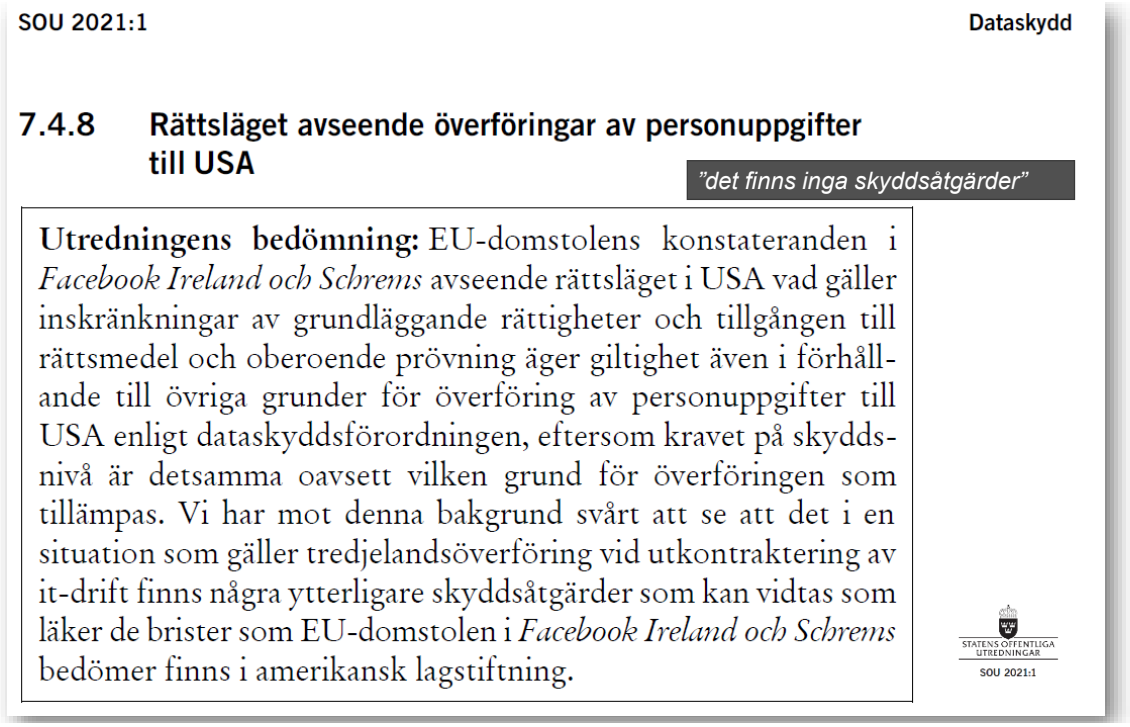


TRAFIKVERKET

Tolkningar utifrån Schrems II från olika auktoriteter

- SOU 2021:1 – Säker och kostnadseffektiv IT-drift (delbetänkande)
- Integritetsskyddsmyndigheten
- ESAMs expertgrupper
- EDPB (Europeiska Dataskyddsstyrelsen)

Trafikverkets agerande ligger i linje med dessa tolkningar.



SOU 2021:1 Dataskydd

7.4.8 Rättsläget avseende överföringar av personuppgifter till USA

”det finns inga skyddsåtgärder”

Utredningens bedömning: EU-domstolens konstateranden i *Facebook Ireland och Schrems* avseende rättsläget i USA vad gäller inskränkningar av grundläggande rättigheter och tillgången till rättsmedel och oberoende prövning äger giltighet även i förhållande till övriga grunder för överföring av personuppgifter till USA enligt dataskyddsförordningen, eftersom kravet på skyddsnivå är detsamma oavsett vilken grund för överföringen som tillämpas. Vi har mot denna bakgrund svårt att se att det i en situation som gäller tredjelandsöverföring vid utkontraktering av it-drift finns några ytterligare skyddsåtgärder som kan vidtas som läker de brister som EU-domstolen i *Facebook Ireland och Schrems* bedömer finns i amerikansk lagstiftning.

STATENS OFFENTLIGA UTREDNINGAR
SOU 2021:1

TRAFIKVERKET

SOU 2021:1 Dataskydd

Det är också vår bedömning att det inte är fråga om en tredjelandsöverföring när personuppgifter behandlas uteslutande inom EU, även om den personuppgiftsansvarige eller personuppgiftsbiträdet som behandlar personuppgifterna är bunden av tredjelands lagstiftning som innebär att denne kan åläggas att lämna ut uppgifter direkt till ett tredjelands myndigheter. Tredjelandsöverföringen sker först i samband med att uppgifterna överförs till myndigheter eller annan mottagare i tredjeland. Däremot kan förekomsten av nämnda skyldigheter enligt vår uppfattning ha betydelse utifrån omsorgsplikten vid val av personuppgiftsbiträde (se avsnitt 7.3.3).

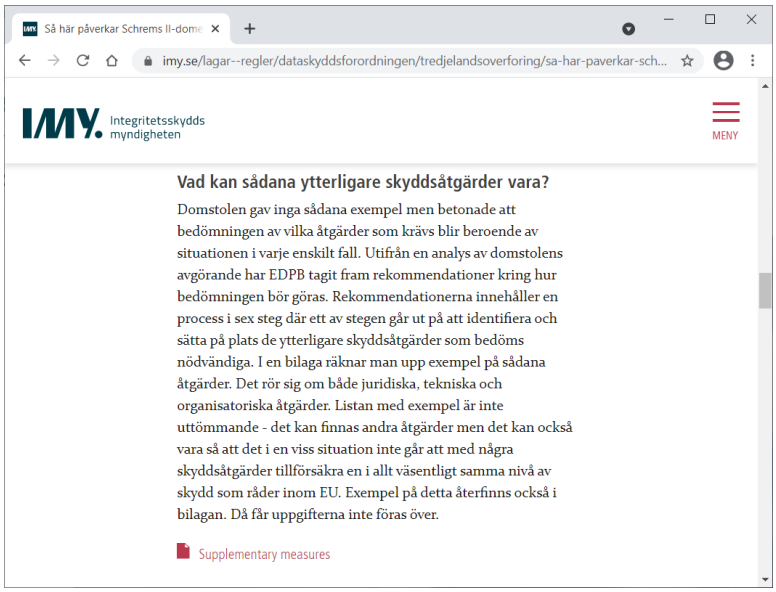
” Omsorgsplikten innebär att man måste välja ett personuppgiftsbiträde som har förmåga att skydda personuppgifterna som behandlas.”

STATENS OFFENTLIGA UTREDNINGAR
SOU 2021:1

TRAFIKVERKET

Hänvisar till Europeiska Dataskydds-styrelsens (EDPB) rekommendationer

EDPB ger exempel på tillräckliga skyddsåtgärder men ribban för dessa ligger högt.



25

2023-02-01

European Data Protection Board

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Adopted on 10 November 2020

Beskriver 6 steg för att hantera utfallet av Schrems II-domen

1) Inventera och se till att endast relevanta data överförs.
2) Verifiera överföringsmekanism.
3) Utvärdera tredjelandets lagstiftning.
4) Utvärdera möjliga skyddsåtgärder.
5) Inför skyddsåtgärder i eller utöver överföringsmekanismen.
6) Omvärdera i lämpliga intervaller.

Uppdaterad version ger exempel på tillräckliga skyddsåtgärder

Länk

26

TRAFIKVERKET

TADPF och Exekutiv order

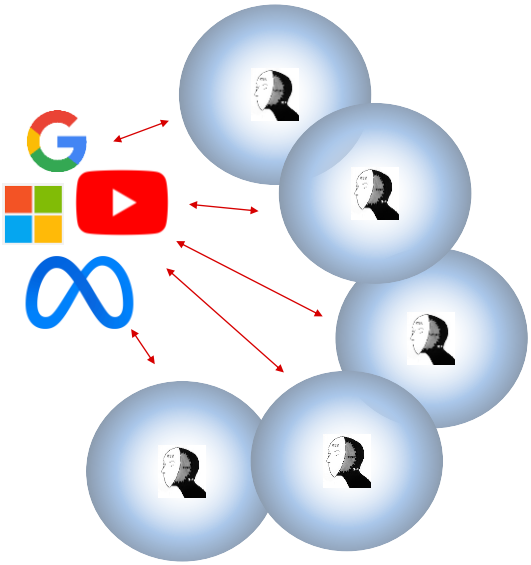
- Trans-Atlantic Data Privacy Framework
- Exekutiv order som stärker mänskliga rättigheter
- På kort sikt: Påverkar TIA Steg 4 i EDPB:s rekommendationer
- På längre sikt: Nytt adekvansbeslut istället för Privacy Shield
- Stabil situation troligen flera år bort

- Ytterligare skyddsåtgärder införs.
- Hanteringskrav för personuppgifter.
- Uppdaterade policies för underrättelsetjänsten
- Granskning- och skadeståndsprocesser införs
- Oberoende granskning införs

Fyra plus en möjliga vägar till ett lagligt läge

28

Privacy i samhällsperspektiv – risk?



- Stora teknikföretag kartlägger individer på detaljerad nivå.
  - Även det undermedvetna
- Används för styrning av annonsflöden och information
  - Filterbubblor
  - Engagemang
  - ?
- Hur påverkar detta samhället?
  - Cambridge Analytica

29

Offentlighet och sekretess

Rättsligt uttalande
2018-10-23
Dnr/ref: VER 2018:57

Rättsligt uttalande om röjande och molntjänster

eSams juridiska expertgrupp har tagit fram detta rättsliga uttalande om behandlingen av sekretessreglerade uppgifter i samband med användningen av vissa typer av molntjänster.

ESAM menar att en uppgifts anses röjd om den tillgängliggörs för en leverantör som lyder under annat lands lagstiftning.

Expertgruppens uttalande

Om sekretessreglerade uppgifter görs tekniskt tillgängliga för en tjänsteleverantör som till följd av ägarförhållanden eller annars är bunden av regler i ett annat land, enligt vilka tjänsteleverantören kan bli skyldig att överlämna information utan att internationell rättshjälp anlitats eller annan laglig grund föreligger enligt svensk rätt, får uppgifterna anses vara röjda. Anledningen är att det inte längre är osannolikt att uppgifterna kan komma att lämnas till utomstående.[1] Detsamma får anses gälla om redan ägarförhållanden eller geografisk placering av en tjänsteleverantörs tekniska hjälpmedel ger anledning att befara att mänskliga rättigheter (till exempel skyddet för privatlivet) eller det allmännas intressen (t.ex. rikets säkerhet) inte skulle säkerställas om svenska myndigheters data hade tillgängliggjorts.

Länk

30

TRAFIKVERKET

Offentlighet och sekretess

8.9 Röjandebegreppet

8.9.1 Lagtexten

Utredningens bedömning: Det följer av lagtexten i offentlighets- och sekretesslagen (2009:400) att ett utlämnande är en form av röjande, att uttrycket röja är ett neutralt begrepp i den meningen att det kan vara såväl tillåtet som otillåtet och att det inte krävs att mottagaren av uppgiften ska ha tagit del av den för att den ska betraktas som röjd.

STATENS OFFENTLIGA UTREDNINGAR
SOU 2021:1

TRAFIKVERKET

Offentlighet och sekretess

8.9.2 Lagmotiven

Utredningens bedömning: Lagmotiven till sekretesslagstiftningen ger ingen närmare vägledning när det gäller frågan hur röjande-begreppet i offentlighets- och sekretesslagen (2009:400) ska tolkas. Det finns i lagmotiven till straffbestämmelsen om brott mot tystnadsplikt i 20 kap. 3 brottsbalken stöd för att en uppgift ska betraktas som röjd så snart den lämnats ut.

STATENS OFFENTLIGA UTREDNINGAR
SOU 2021:1

TRAFIKVERKET

AFC.25 Beställarens krav på sekretess (1/2)

Trafikverket i egenskap av förvaltningsmyndighet lyder under den svenska offentlighetsprincipen. Det innebär att tredje man har rätt att ta del av allmänna handlingar hos Trafikverket, förutom uppgifter

- //Uppgift som lämnar eller kan bidra till upplysning om **säkerhets- eller bevakningsåtgärd**, där det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser byggnader eller andra anläggningar, lokaler eller inventarier (18 kap. 8 § 1 OSL).//
- //Uppgift som hänför sig till en myndighets verksamhet som **består i risk- och sårbarhetsanalyser** avseende fredstida krissituationer, planering och förberedelser inför sådana situationer eller hantering av sådana situationer, där det kan antas att det allmännas möjligheter att förebygga och hantera fredstida kriser motverkas om uppgiften röjs (18 kap. 13 § OSL).//
- //**Uppgift om en djur- eller växtart som är i behov av skydd** och som det finns ett intresse av att bevara i ett livskraftigt bestånd, där det kan antas att ett sådant bevarande av arten inom landet eller del av landet motverkas om uppgiften röjs (20 kap. 1 § OSL).//
- //?//

TRAFIKVERKET

AFC.25 Beställarens krav på sekretess (2/2)

Trafikverket åtar sig att markera var uppgifterna finns och när uppgifterna framförs muntligt.

Entreprenören åtar sig att inte utan Trafikverkets godkännande **ge tredje man, inklusive underentreprenörer, leverantörer och andra avtalsparter, tillgång vare sig skriftligt eller muntligt till uppgifterna**. Skyldigheten gäller utan begränsning av tider, tidsfrister eller liknande i kontrakts-, entreprenad- eller övriga handlingar. Skyldigheten gäller inte uppgifter som redan är allmänt kända eller som måste lämnas ut enligt lag.

Entreprenören åtar sig att se till att alla fysiska personer som arbetar under entreprenörens ledning och får eller kan antas få kännedom om uppgifterna är bundna av sekretessförbindelser som motsvarar det föregående stycket och, om Trafikverket begär det, ingår individuella sekretessförbindelser med Trafikverket.

Entreprenören åtar sig att se till att tredje man, inklusive underentreprenörer, leverantörer och andra avtalsparter, som godkänts av Trafikverket enligt ovan, samt alla fysiska personer som arbetar under dessa aktörers ledning och som får eller kan antas få kännedom om uppgifterna, är bundna av motsvarande sekretessförbindelser.//

TRAFIKVERKET

Sekretesstolkningar i IT-driftsutredningen

Vilka tjänster som kan användas beror skaderekvisit (nivå av sekretess)

STATENS OFFENTLIGA UTREDNINGAR
SOU 2021:1

35

Sekretessgenombrott vid teknisk bearbetning eller lagring av uppgifter

I lagrådsremissen föreslås en ny sekretessbrytande bestämmelse som möjliggör för myndigheter att lämna uppgifter som omfattas av sekretess till en enskild eller till en annan myndighet som har i uppdrag att tekniskt bearbeta eller tekniskt lagra uppgifterna för den uppgiftslämnande myndighetens räkning.

- **Teknisk bearbetning och lagring är begränsat**
- **Lämplighetsbedömning krävs**
- **Undantag från meddelarfrihet**

Tänkt att börja gälla 1 juli 2023 och är inte ett frikort för molntjänster

Länk

36

Offentlighet och sekretess

- Trafikverkets förhållningssätt är inte välfungerande och behöver förbättras.
- Lägg inte uppgifter som berörs av sekretess i molntjänster.

37

Digital suveränitet och beredskap

STATENS OFFENTLIGA UTREDNINGAR

SOU 2021:97

Säker och kostnadseffektiv it-drift

38

TRAFIKVERKET

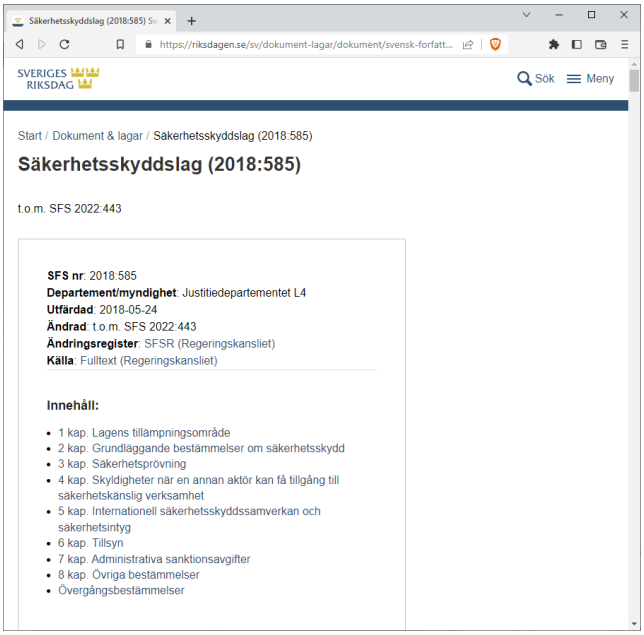
Digital suveränitet – perspektiv

- Rådighet över egna informationstillgångar. Industrispionage?
- Fråga om nationell säkerhet.
- IT-driftsutredningens slutbetänkande.
- Trafikverket är en beredskapsmyndighet.
- Leverantörsinlåsning.
- Alla ägg i ett fåtal korgar?
- Är molntjänster verkligen säkrare och billigare?
- Integrationsmöjligheter via öppna format och protokoll.
- Exit från molntjänster.

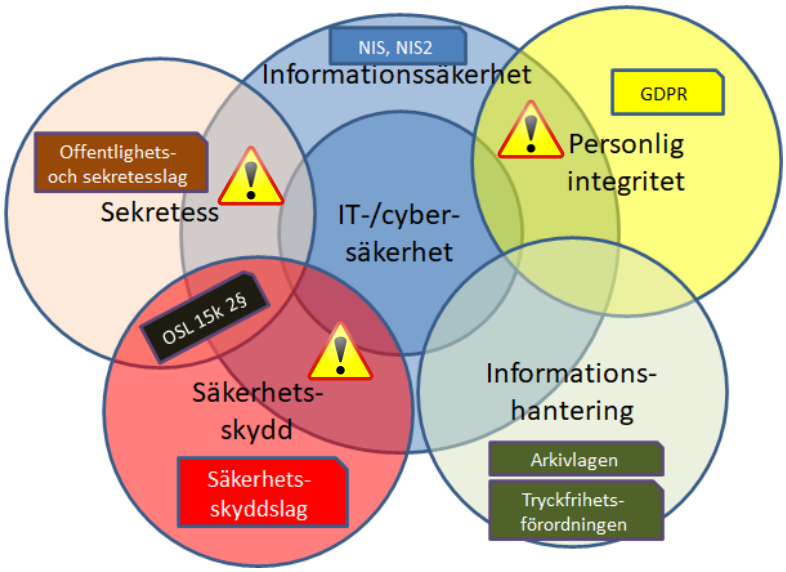
TRAFIKVERKET

Säkerhetsskydd

- Korrekt men ineffektiv hantering av säkerhetsskyddslagen
- Säkerhetsskyddavtal
- Personkontroller
- Informationsklassning
- ”Hemliga datorer”
  - Svårförvaltade
  - En säkerhetsskyddad projekteringsmiljö hade varit önskvärd



TRAFIKVERKET



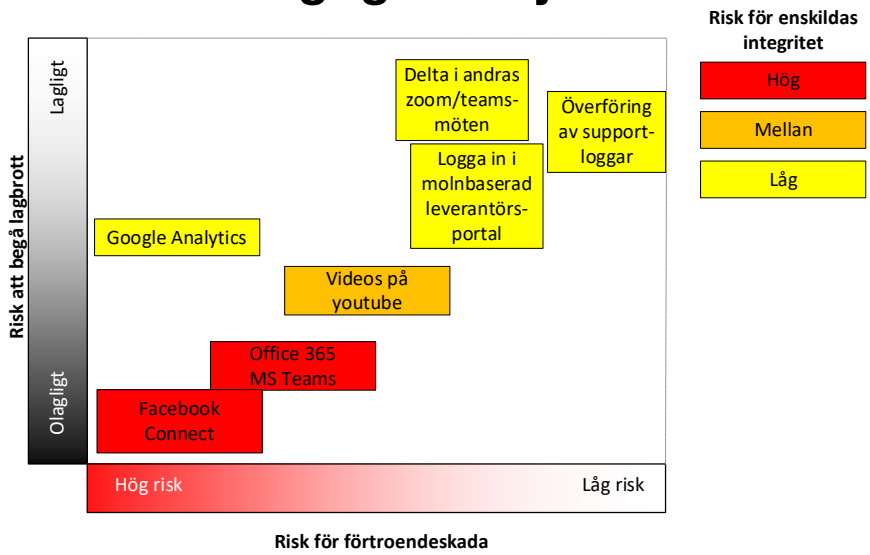
TRAFIKVERKET

Digitalisering av bygg- och anläggning

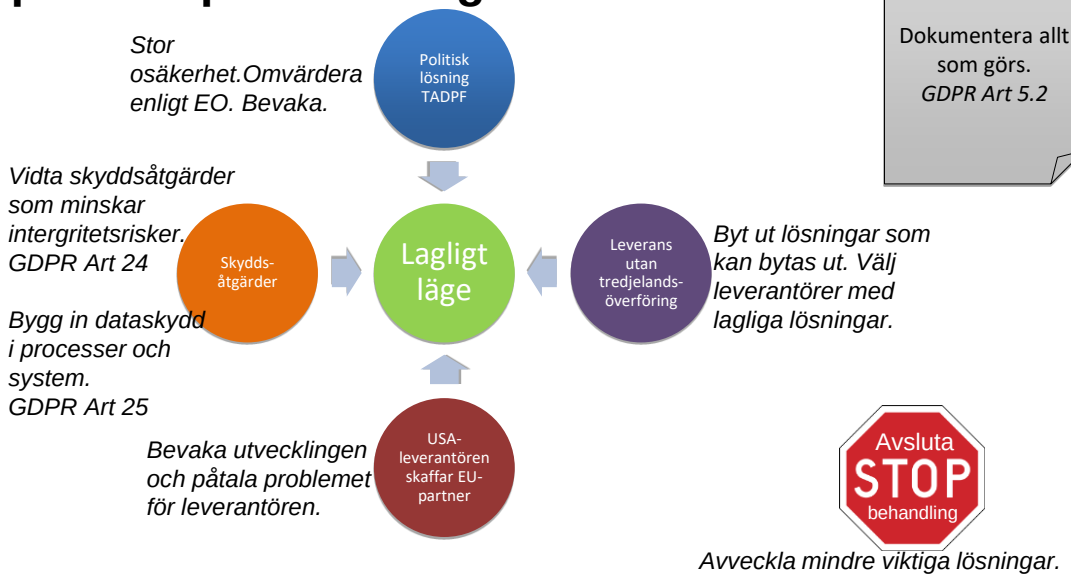
Trafikverkets utmaning och förhållningssätt

TRAFIKVERKET

Risker med olagliga tredjelandsöverföringar



Arbeta på alla spår samtidigt



44

Trafikverkets molngrupp

Tvärfunktionell grupp som ger råd i frågor om användning av molntjänster

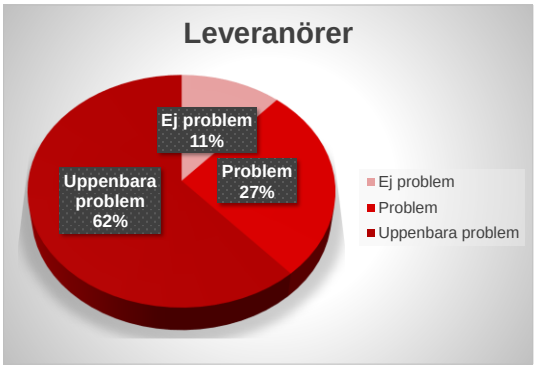
- Ingen fixerat internt regelverk än så länge
- Individuell bedömning av varje molntjänst
- Helhetsperspektiv på juridisk risk
- Begäran om GDPR-information (Art 12-14)
- Viktiga lösningar = juridisk risk kan tolereras tills vidare
- ”Nice to have” = noll tolerans för juridisk risk

TRAFIKVERKET

Fråga till A- och B-leverantörer

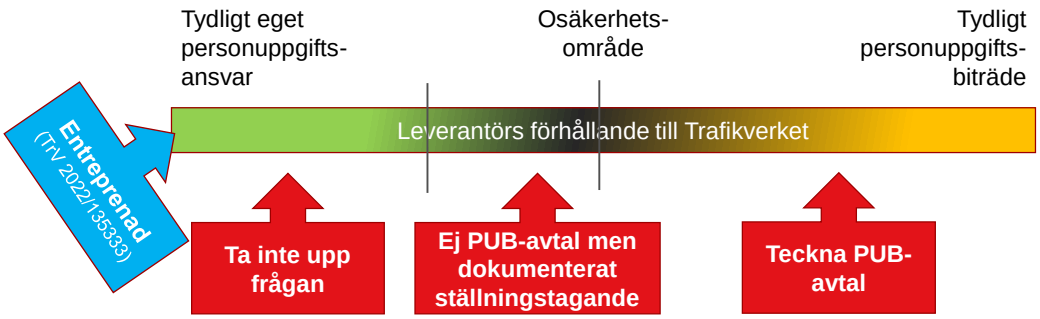
I januari tillfrågades samtliga A- och B-leverantörer hurvida de var drabbade av Schrems II-problematik. De 26 svar som kom in bedömdes enligt följande.

- 3 leverantörer indikerar inga problem.
- 7 leverantörer indikerar problem.
- 16 leverantörer indikerar uppenbara problem



TRAFIKVERKET

Strategi för personuppgiftsbiträdesavtal



- Inga PUB-avtal för ”säkerhets skull”.
- Ställningstaganden bevakas då rättsläget är osäkert.
- Ställningstagande om PUB tas i samband med avtal – ej i upphandling.
- Detta beskrivs i TDOK 2018:0474
- Diarieför som bilaga till huvudavtal
  - Metadatat ”åtgärd/handling” sätts till ”personuppgiftsbiträdesavtal”

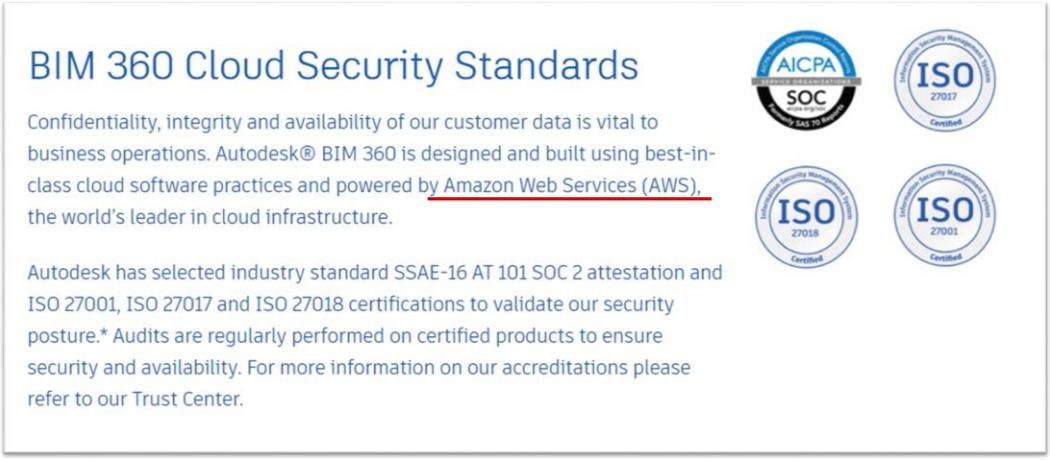
47

Verksamhet hos leverantörer

- Personuppgiftsansvariga bär själva det juridiska ansvaret.
  - Anställdas uppgifter
    - Trafikverksanställda
    - Leverantörer till Trafikverket
  - Tredje parts uppgifter
    - Allmänhet
    - Intressenter
- För personuppgiftsbiträden bär Trafikverket det juridiska ansvaret.

48

Marknadsledare inom entreprenad bygger på molntjänster



49

Marknadsledare inom entreprenad bygger på molntjänster

50

Riskbild PUB - Entreprenad

- SOU 2021 och EDPB riktlinje för personuppgiftsansvariga och personuppgiftsbiträden att kan tolkas som att myndigheter i princip alltid är personuppgiftsansvariga för all sin egen och upphandlad verksamhet.
- I informellt samtal med IMY bedömdes Trafikverkets nuvarande bedömning som ”inte orimlig”.
- Trafikverket bör fortsätta med nuvarande bedömning, men behöver notera den juridiska risken samt övrig problematik.
  - Personuppgifter hamnar i molntjänster
  - Sekretessbelagd information i molntjänster?

51

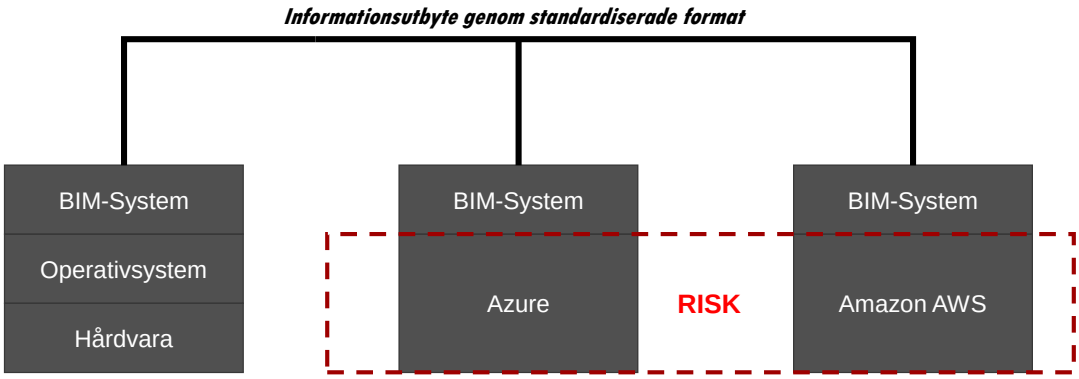
TRAFIKVERKET

Industry Foundation Classes
(ISO 16739-1:2018)
Fritt och öppet datautbytesformat (CC-BY-ND).

IFC

CoClass

CoClass är samhällsbyggarnas gemensamma klassifikationssystem för framtidssäkrad dokumentation.



52

TRAFIKVERKET

Hur skall Trafikverket hantera våra entreprenadleverantörer som använder molntjänster

- Kan Trafikverket tolerera att personuppgifter hanteras olagligt?
- Behandlas sekretessbelagda uppgifter i molntjänster?
  - Uppgifter som kommer från Trafikverket?
  - Uppgifter som leverantören upprättar?
- Vad är alternativen?
  - Bygga upp en egen projekteringsmiljö?
- Vad blir konsekvenserna om vi förbjuder våra leverantörer att använda molntjänster?
- **Om Trafikverket tecknar personuppgiftsbiträdesavtal med entreprenörer blir Trafikverket ansvariga för alla olagliga tredjelandsöverföringar.**